Generalizations of Bent Functions. A Survey [1]

Natalia Tokareva

Sobolev Institute of Mathematics
Novosibirsk, Russia

tokareva@math.nsc.ru

Bent functions (Boolean functions with extreme nonlinearity properties) are actively studied for their numerous applications in cryptography, coding theory, and other fields. New statements of problems lead to a large number of generalizations of the bent functions many of which remain little known to the experts in Boolean functions. In this article, we offer a systematic survey of them.

Keywords: Boolean function, nonlinearity, bent function, generalized bent function

Introduction

The term a *generalized bent function* is used quite often, but almost every time it means something new. Bent functions are actively studied for their numerous applications in information theory, cryptography, coding theory, and other fields. New statements of problems lead to many generalizations of bent functions, and it becomes more and more difficult to clear it up.

In this article we offer a systematic survey of the existing generalizations of bent functions and try whenever possible to establish relations between various generalizations. This article can be regarded as a continuation of the survey [17]. We assume that the reader is familiar with the main results concerning bent functions.

We divide the generalizations of bent functions into several groups. Note right away that the division is somewhat vague, but it seems convenient for the presentation. While describing each generalization, we pay attention if possible to who, when, and why introduced this generalization; what is the form of the functions and the Walsh–Hadamard (or Fourier) transform occurring as a rule in each case; what are the available results; how this generalization is related to others, and so forth. For every generalization, we include appropriate references.

Let us present the structure of the article.

Section 1: Algebraic generalizations of bent functions (q-valued bent functions; bent functions over a finite field; generalized Boolean bent functions; bent functions on a finite abelian group with values in the set of complex numbers on the unit circle; bent functions on a finite abelian group with values in another finite abelian group; vector G-bent functions; multidimensional bent functions on a finite abelian group).

[1] This is an English translation of the paper published in Russian Journal *Discrete Analysis and Operation Research* [Diskretn. Anal. Issled. Oper.] 2010. V. 17. N 1. P. 34-64.

Section 2: Combinatorial generalizations of bent functions (partially defined bent functions; plateaued functions; $\mathbb{Z}$-bent functions; homogeneous bent functions).

Section 3: Cryptographic generalizations of bent functions (balanced bent functions; partial bent functions; hyper-bent functions; near-bent functions; order r bent functions; k-bent functions).

Section 4: Quantum generalizations of bent functions (negabent functions; bent$_4$-functions; I-bent functions).

Let us list the notation and definitions:

q and n are positive integers;

$+$ stands for the addition modulo q;

$x = (x_1, \ldots, x_n)$ is a q-valued vector;

$\mathbb{Z}_q^n$ is the set of all q-valued vectors of length n;

$\mathbb{F}_{q^n}$ is the Galois field of order q^n;

$\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$ is the inner product of vectors;

$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is a Boolean function of n variables;

$W_f(y) = \sum_{x\in\mathbb{Z}_2^n}(-1)^{\langle x,y\rangle+f(x)}$ is the Walsh–Hadamard transform of a Boolean function f;

N_f is the *nonlinearity* of a Boolean function f; i.e., the Hamming distance from f to the set of all affine functions;

a *bent function* (for even n) is a Boolean function all of whose Walsh–Hadamard coefficients are equal to $\pm 2^{n/2}$;

$\mathfrak{B}_n$ is the class of bent functions of n variables.

1. Algebraic generalizations of bent functions

In this section we collect the generalizations in which the functions considered are not Boolean functions. As a rule, these are the mappings between some algebraic systems.

1.1. The q-Valued Bent Functions

In 1985, P. V. Kumar, R. A. Scholtz, and L. R. Welch proposed [37] this natural generalization of bent functions, aiming to construct q-valued bent sequences applicable in CDMA systems (see more details below).

Take integer $q \geqslant 2$, the imaginary unit $i = \sqrt{-1}$, and a primitive complex root of unity $\omega = e^{2\pi i/q}$ of degree q. Consider the q-valued function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$.

The *Walsh–Hadamard transform* of a function f is the complex function

$$W_f(y) = \sum_{x\in\mathbb{Z}_q^n} \omega^{\langle x,y\rangle+f(x)} \quad \text{for every} \quad y \in \mathbb{Z}_q^n, \tag{1}$$

where the inner product and addition $+$ are taken modulo q.

Denote the absolute value of a complex number c by $|c|$.

Definition 1 (Kumar, Scholtz and Welch, 1985). Given positive integer q, a function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called a *q-valued bent function* if $|W_f(y)| = q^{n/2}$ for every $y \in \mathbb{Z}_q^n$.

For $q = 2$, this concept coincides with the concept of a Boolean bent function. Denote the set of all q-valued bent functions of n variables by $\mathfrak{B}_{n,q}$. The following is obtained in [37]:

Theorem 1. *The class $\mathfrak{B}_{n,q}$ is closed under*
(i) *every nondegenerate affine transformation of the variables;*
(ii) *addition of arbitrary q-valued affine functions.*

A square $n \times n$-matrix A consisting of integer powers of ω is called a *generalized Hadamard matrix* whenever $A\overline{A}^T = nE$, where E is the identity matrix.

Theorem 2. *The following are equivalent:*
(i) *a q-valued function f is a bent function;*
(ii) *the matrix $A = (a_{x,y})$ with $a_{x,y} = \omega^{f(x+y)}$ is a generalized Hadamard matrix.*

Note that, for $q = 2$, Theorems 1 and 2 amount to well-known facts on Boolean bent functions (for instance, see [17]). The specific features of the q-valued case include the fact [37] that f remains a bent function when we replace ω in the definition of $W_f(y)$ by another primitive root of unity γ of degree q. Note also that q-valued bent functions exist both for even and odd n.

Theorem 3. *Take arbitrary positive integers m, n, and q. For arbitrary functions $g \in \mathfrak{B}_{m,q}$ and $h \in \mathfrak{B}_{n,q}$, the function $f(x', x'') = g(x') + h(x'')$ is a q-valued bent function.*

An analog of Maiorana–McFarland theorem [40] holds:

Theorem 4. *If n is even and q is arbitrary then*

$$f(x', x'') = \langle x', h(x'')\rangle + g(x'')$$

is a q-valued bent function, where g is an arbitrary q-valued function of $n/2$ variables, and h is an arbitrary permutation on the set $\mathbb{Z}_q^{n/2}$.

Suppose that n is odd, $q = 2 \bmod 4$ and $q > 2$. It is shown in [37] that if there exists an integer b such that $2^b + 1$ is divisible by $q/2$ then there exists no q-valued bent function of n variables.

Bent functions exist for every q with $q \neq 2 \bmod 4$ and every n. They can be constructed using Theorem 3, for instance, from the following one-dimensional functions ($n = 1$):

Theorem 5. *The following q-valued functions of one variable are bent functions:*
(i) *$f(x) = x^2 + cx$, where $c \in \mathbb{Z}_q$ is an arbitrary constant (if q is odd);*
(ii) *$f(x) = rx'h(x'') + g(x'')$, where $x = rx' + x'' \in \mathbb{Z}_q$, $0 \leqslant x', x'' \leqslant r - 1$, h is an arbitrary permutation on $\mathbb{Z}_r$, and g is an arbitrary function of the form $\mathbb{Z}_r \to \mathbb{Z}_q$ (if $q = r^2$ for some r).*

See [37] for more details. X. D. Hou proposed [35] some constructions of q-valued bent functions obtained using chain rings:

Regular q-valued bent functions retain the properties of Boolean bent functions most completely. A bent function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called *regular* if each of its Walsh–Hadamard coefficients can be expressed as

$$W_f(y) = q^{n/2}\omega^{g(y)}$$

for some q-valued function g. It can be shown [37] that g is also a regular bent function and is called the *dual* to f.

Let us give several examples:

• For $n = 1$ and $q = 4$, $f(x) = x^3 + 3x^2$ is a regular bent function. Its Walsh–Hadamard spectrum (the tuple of coefficients in the increasing order of arguments) is

$$(2, 2i, 2, -2i) = (2\omega^0, 2\omega^1, 2\omega^0, 2\omega^3),$$

where $\omega = e^{\pi i/2}$; the dual function $g(x)$ is equal to x^3.

• For $n = 1$ and $q = 3$, the bent function $f(x) = x^2$ is not regular; its spectrum is equal to

$$\left\{\sqrt{3}i,\ \frac{3}{2} - \frac{\sqrt{3}}{2}i,\ \frac{3}{2} - \frac{\sqrt{3}}{2}i\right\}$$

or, using the powers of a primitive root of unity,

$$\{\sqrt{3}\omega^{3/4},\ \sqrt{3}\omega^{11/4},\ \sqrt{3}\omega^{11/4}\},$$

where $\omega = e^{2\pi i/3}$. Here all exponents in the powers of ω are fractional.

It is not difficult to observe that a Boolean bent function ($q = 2$) is always regular. The bent functions constructed in Theorems 4 and 5 (for $q = 1 \bmod 4$ in claim (i)) are regular. For odd n and $q = 2, 3 \bmod 4$, no regular bent function exists [37]. S. V. Agievich showed [19] that regular q-valued bent functions can be described using *bent rectangles*; in the binary case, this description appears in [17].

The q-valued bent functions for $q = 4$ are studied in [56]. We can express an arbitrary quaternary function f of n variables as $f(x+2y) = a(x, y)+2b(x, y)$ with suitable Boolean functions a and b of $2n$ variables, where $x, y \in \mathbb{Z}_2^n$.

Boolean functions c and d of $2n$ variables are called *bent correlating* (for a given subdivision of the set of variables into two equal parts) if, for every $x, y \in \mathbb{Z}_2^n$, the following conditions are fulfilled:

(i) $W_c^2(x, y) + W_c^2(x + y, y) + W_d^2(x, y) + W_d^2(x + y, y) = 4^{n+1}$;

(ii) $W_c(x, y) = W_d(x + y, y) = \pm 2^n \iff W_c(x + y, y) = W_d(x, y) = \pm 2^n$.

If c and d are bent functions then (i) is always fulfilled. Condition (ii) determines a certain agreement of signs of the Walsh–Hadamard coefficients of these functions. Note that the bent correlating functions either are or are not bent functions simultaneously. The next theorem is proved in [56].

Theorem 6. *A function $f : \mathbb{Z}_4^n \to \mathbb{Z}_4$ is a bent function in the sense of Definition 1 if and only if b and $a + b$ are bent correlating functions.*

For more on q-valued bent functions, see [34, 36]; and on bent-sequences, [44].

1.2. Bent Functions over a Finite Field

In 1994, A. C. Ambrosimov proposed [2] another, probabilistic definition of q-valued bent functions. In contrast to the previous case, here we consider only the q-valued functions over the finite field $\mathbb{F}_{q^n}$.

Suppose that $q = p^\ell$, where p is prime and ℓ is positive integer. Take the primitive complex root of unity $\omega = e^{2\pi i/p}$ of degree p.

Take a q-valued function $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Assume that a vector $x \in \mathbb{F}_{q^n}$ is chosen randomly and with equal probabilities. For the random variable $\xi = f(x)$, define the characteristic function

$$\varphi_\xi(z) = \mathbf{E}\, \omega^{\langle \xi, z\rangle}, \qquad z \in \mathbb{F}_q,$$

regarding ξ and z as vectors of length ℓ over the prime field $\mathbb{F}_p$ and taking the inner product $\langle \xi, z\rangle$ modulo p. For fixed $z \in \mathbb{F}_q$, the *Walsh–Hadamard transform* of f is defined as

$$W_{f,z}(y) = q^n\ \varphi_{\langle x,y\rangle + f(x)}(z),$$

or, which is the same,

$$W_{f,z}(y) = q^n\ \mathbf{E}\, \omega^{\langle \langle x,y\rangle + f(x), z\rangle} \quad \text{for every} \quad y \in \mathbb{F}_{q^n},$$

where we take the inner product $\langle x, y\rangle$ modulo q. Expanding the expectation, we obtain

$$W_{f,z}(y) = \sum_{x \in \mathbb{F}_{q^n}} \omega^{\langle \langle x,y\rangle + f(x), z\rangle} \quad \text{for} \quad y \in \mathbb{F}_{q^n}. \tag{2}$$

Note that in (1) and (2) we use the primitive roots of unity of different degrees q and p respectively. The parameter z in (2) determines the projection of $\langle x, y\rangle + f(x)$ from $\mathbb{F}_q$ to the prime field $\mathbb{F}_p$.

We can propose an equivalent definition

$$W'_{f,z}(y) = \sum_{x \in \mathbb{F}_{q^n}} \omega^{\mathrm{Tr}(\langle x,y\rangle + z f(x))}$$

replacing the inner product by the trace function $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$. With this definition, $W_{f,z}(y)$ and $W'_{f,z}(y)$ differ only up to a permutation on the components of z and y.

According to [2], every function f and every nonzero z satisfy Parseval's equality

$$\sum_{y \in \mathbb{F}_{q^n}} |W_{f,\,z}(y)|^2 = q^{2n},$$

which implies

$$\max_{y \in \mathbb{F}_{q^n}} |W_{f,z}(y)| \geqslant q^{n/2}.$$

Definition 2 (Ambrosimov, 1994). Take $q = p^\ell$ with prime p. A function $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is called a *bent function* if, for all vectors $z \in \mathbb{F}_q \backslash \{0\}$ and $y \in \mathbb{F}_{q^n}$,

$$|W_{f,\,z}(y)| = q^{n/2}.$$

Let us make some remarks:

• For $q = p$ and $\ell = 1$, Definition 2 of q-valued bent functions coincides with Definition 1 of Kumar, Scholtz and Welch.

• In Definition 2, the Walsh–Hadamard coefficients must be equal in absolute value for every nonzero projection of the exponent of the power of the primitive element in (2) from $\mathbb{F}_q$ to the field $\mathbb{F}_p$. Then, as in Definition 1, they are equal

in absolute value without considering the projections (moreover, $\mathbb{Z}_q$ need not be a field).

Let us present several examples. Every q-valued function $f(x) = a_2x^2 + a_1x + a_0$ of one variable, where $a_2 \neq 0$ and $p \neq 2$, is a bent function in the sense of Ambrosimov. Every function $f(x_1, x_2) = x_1x_2 + a_2x_1^2 + b_2x_2^2 + a_1x_1 + b_1x_2 + c$ of two variables over a field of characteristic 2 is a bent function.

For bent functions over a field, we have Rothaus' criterion [2]:

Theorem 7. *A function $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is a bent function if and only if, for every fixed $y \in \mathbb{F}_{q^n}$, the function $f(x + y) - f(x)$ is uniformly distributed on $\mathbb{F}_q$ whenever the argument x is uniformly distributed on $\mathbb{F}_{q^n}$.*

A description of all quadratic q-valued bent functions of n variables appears in [2], where their number is also calculated, which we denote by $M_q(n)$.

Theorem 8. *Take $q = p^\ell$. The following hold:*
(i) *if $p = 2$ and $\ell \geqslant 2$ then*

$$M_q(n) = \begin{cases} q^{\binom{n}{2}+2n+1} \prod\limits_{j=1}^{n/2}(1 - q^{-2j+1}), & \text{for even } n, \\ 0, & \text{for odd } n; \end{cases}$$

(ii) *if $p \neq 2$ then*

$$M_q(n) = (q-1)q^n M_q(n-1) + q^{n+1}(q^{n-1} - 1)M_q(n-2) \quad \text{for} \quad n \geqslant 3.$$

Unfortunately, [2] fails to trace explicitly the relationships between the Ambrosimov's bent functions and those of Kumar, Scholtz, and Welch. For $q = p^\ell$, it is not clear, for instance, whether a bent function in one sense is a bent function in the other.

1.3. Generalized Boolean Bent Functions of Schmidt

In 2006, K.-U. Schmidt considered [55] another generalization of bent functions in connection with a construction of quaternary constant-amplitude codes for multicode CDMA systems. Let us dwell on this in more detail.

The CDMA (Code Division Multiple Access) technology for digital mobile service was standardized in 1993 by the US Telecommunication Industry Association (US TIA) as the standard IS–95 (Mobile Station–Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System). Presently the technology is actively used by the majority of mobile equipment providers throughout the world in accordance with the third generation mobile service standard IMT–2000 (in Russia, the standard IMT–MC 450 or CDMA–450). Note that the first article [1] devoted to this technology was published in USSR already in 1935 by D. V. Ageev. The CDMA systems use broadband signals, and many clients simultaneously use the whole band of frequencies of the channel. Since every client is assigned a unique code, it is easy to isolate this

code from the "noise." The CDMA systems substantially increase the bandwidth of the channel and are quite efficient.

In 2000, T. Wada established [57] a connection between bent functions and codes for CDMA (see also the articles by K. G. Paterson [47]).

Consider the simplest model of information transmission in a multicode CDMA system. For a power of two $N = 2^n$, take a size $N \times N$ Hadamard matrix $A_N = (a_{jt})$ of Sylvester's type. There are N parallel data flows. We can represent the transmitted information as a binary vector c of length N (one bit from each flow). The signal in MC-CDMA is modelled as

$$S_c(t) = \sum_{j=0}^{N-1} (-1)^{c_j} a_{jt},$$

where $t = 0, 1, \ldots, N-1$ is a discrete time parameter; i.e., the jth row of the matrix A is multiplied by $(-1)^{c_j}$, and the transmitted signal S_c is the sum of these new rows. At every moment of time, one bit of the sequence S_c is transmitted. An important parameter is the *peak-to-average power ratio* of the signal, which is defined as

$$\mathrm{PAPR}(c) = \frac{1}{N} \max_t |S_c(t)|^2.$$

Note that $1 \leqslant \mathrm{PAPR}(c) \leqslant N$. The quantity $|S_c(t)|^2$ is proportional to the power necessary to transmit this signal; thus, the vectors c with minimal $\mathrm{PAPR}(c)$ are most suitable for transmission. We may assume that the vectors c are chosen from some binary code C of length N. Put

$$\mathrm{PAPR}(C) = \max_{c \in C} \mathrm{PAPR}(c).$$

If $\mathrm{PAPR}(C) = 1$ then C is called a *constant amplitude code*. Currently it is a problem to construct a code of this type with large size and large code distance. We have [47, 57]

Theorem 9. *A code C of length 2^n is a constant amplitude code if and only if every code word is a vector of values of some bent function of n variables.*

Indeed, given the vector c of values of a Boolean function f of n variables,

$$\mathrm{PAPR}(c) = \frac{1}{2^n} \max_{x \in \mathbb{Z}_2^n} |W_f(x)|^2.$$

Therefore, bent functions play a substantial role in constructing codes for CDMA systems.

The generalization [55] due to K.-U. Schmidt goes as follows:

For an integer $q \geqslant 2$, take a primitive complex root of unity $\omega = e^{2\pi i/q}$ of degree q. A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ is called a *generalized Boolean function*. Refer as its *Walsh–Hadamard transform* to the complex function

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x,y \rangle} \omega^{f(x)} \quad \text{for every} \quad y \in \mathbb{Z}_2^n.$$

Definition 3 (Schmidt, 2006). For positive integer q, a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ is called a *generalized bent function* if $|W_f(y)| = 2^{n/2}$ for every $y \in \mathbb{Z}_2^n$.

These functions are used for constructing the constant amplitude codes for the q-valued version of MC–CDMA, which models a binary vector c of length N as

$$S_{c,q}(t) = \sum_{j=0}^{N-1} \omega^{c_j} a_{jt}.$$

Note also that, for some problems concerning cyclic codes, Schmidt's definition seems more natural than the definition of q-valued bent functions by Kumar, Scholtz, and Welch.

Schmidt deals in detail [55] with the case $q = 4$, studies the relations between generalized bent functions, constant amplitude codes, and the available $\mathbb{Z}_4$-linear codes.

An interesting question remains: how related to each other are the bent functions of Schmidt, the q-valued, and the Boolean bent functions? This question is answered in [56] in one particular case. Suppose that a generalized Boolean function $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$ ($q = 4$) can be presented as $f(x) = a(x) + 2b(x)$, where a and b are Boolean functions of n variables. It is shown in [56] that f is a generalized bent function if and only if b and $a + b$ are ordinary bent functions.

Note that the *real-valued bent functions* of the form $\mathbb{Z}_2^n \to \{0, 1/2, 1, 3/2\}$ considered in [41] coincide with the generalized bent functions for $q = 4$.

1.4. Bent Functions from a Finite Abelian Group into the Set of Complex Numbers on the Unit Circle

In 1997, O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko introduced [10] the concept of bent functions on an arbitrary finite abelian group. In the case of an elementary abelian 2-group, this concept coincides with the concept of Boolean bent functions.

Take a finite abelian group $(A, +)$ of order n the maximal order of whose elements (the *exponent* of the group) is equal to q. Denote the group of degree q roots of unity by

$$T_q = \{e^{2\pi ik/q} \mid k = 0, 1, \ldots, q-1\},$$

and the group of homomorphisms $\chi : A \to T_q$, by $\widehat{A}$, which is called the *character group* of A (or its *dual group*). It is known that A and $\widehat{A}$ are isomorphic. Fix some isomorphism $y \in A$, $y \to \chi_y$.

Instead of the Walsh–Hadamard transform it is convenient to introduce the *Fourier transform* of a complex valued function $f : A \to \mathbb{C}$ as

$$\widehat{f}(y) = \sum_{x \in A} f(x)\overline{\chi_y(x)}.$$

Henceforth, we consider only the functions from A into $\mathbb{C}$ all of whose values lie on the unit circle $S_1(\mathbb{C})$ centered at the origin.

Definition 4 (Logachev, Sal'nikov, and Yashchenko, 1997). Take a finite abelian group A of order n. A function $f : A \to S_1(\mathbb{C})$ is called a *bent function* if $|\widehat{f}(y)|^2 = n$ for every $y \in A$.

Let us make the following remarks:

• If A is an elementary abelian 2-group, i.e., $q = 2$ and $n = 2^m$ for some positive integer m, then this concept coincides with the concept of ordinary bent functions of m variables.

• Take two integers q and m. Then the q-valued bent functions of m variables of Kumar, Scholtz, and Welch (see Definition 1) constitute a particular case of the bent functions of Definition 4 with $A = \mathbb{Z}_q^m$ and $n = q^m$, but a little modification is necessary: from the functions of the form $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ we have to pass to the functions $f' : \mathbb{Z}_q^m \to T_q \subset \mathbb{C}$, where $f'(x) = \omega^{f(x)}$. As an isomorphism between A and its character group $\widehat{A}$ choose the correspondence $y \to \chi_y(x) = \omega^{\langle x,y\rangle}$, where $\omega = e^{2\pi i/q}$.

A function $f : A \to S_1(\mathbb{C})$ is called *balanced* whenever

$$\sum_{x\in A} f(x) = 0.$$

The following is the Rothaus criterion for bent functions on a group [10]:

Theorem 10. *A function f is a bent function on the group A if and only if $\overline{f(x)}f(x+y)$ is balanced for every $y \in A$, $y \neq 0$.*

Some other criteria can be found in [10].

As in the case of a Boolean function, for a bent function f on a group A, we can define the *dual* function $\widetilde{f} : A \to S_1(\mathbb{C})$ by

$$\widetilde{f}(x) = \frac{1}{\sqrt{n}}\ \widehat{f}(x),$$

and $\widetilde{f}$ is a bent function as well.

If, for a decomposition of A into the direct product of some groups A_1 and A_2, we can express a function $f : A \to S_1(\mathbb{C})$ as

$$f(x', x'') = f_1(x')f_2(x''),$$

where $f_1 : A_1 \to S_1(\mathbb{C})$ and $f_2 : A_2 \to S_1(\mathbb{C})$, then f is called a *decomposable* function. We have [10]

Theorem 11. *A decomposable function f is a bent function on the group A if and only if f_1 and f_2 are the bent functions on the groups A_1 and A_2 respectively.*

1.5. Bent Functions from a Finite Abelian Group into Another Finite Abelian Group

In 2002, V. I. Solodovnikov proposed [13] the most general approach to algebraic generalizations of bent functions. While presenting his results, we use both the original notation and that of [24] which sometimes seems more convenient. In 2004, C. Carlet and C. Ding repeated [24] the results of Solodovnikov, unfortunately, without a reference to his work.

Take two finite abelian groups $(A, +)$ and $(B, +)$ of orders n and m respectively, with the maximal orders a and b of their elements. Let $\widehat{A}$ and $\widehat{B}$ denote the character groups of A and B. Fix two isomorphisms $y \to \chi_y$ and $z \to \eta_z$

between A and $\widehat{A}$, as well as B and $\widehat{B}$, where $\chi_y : A \to T_a$ and $\eta_z : B \to T_b$ are characters. Take an arbitrary function $f : A \to B$. We present the following definition of [13] in a slightly different form by introducing normalization factors, but this preserves their meaning.

Refer as the *Fourier transform* of the character of a function f for fixed $z \in B$ to the function

$$\widehat{f}_z(y) = \sum_{x \in A} \eta_z(f(x))\overline{\chi_y(x)}, \qquad y \in A. \tag{3}$$

Parseval's equality $\sum\limits_{y \in A} |\widehat{f}_z(y)|^2 = n^2$ holds for every z.

Definition 5 (Solodovnikov, 2002). A function $f : A \to B$ is called a *bent function* if $|\widehat{f}_z(y)|^2 = n$ for every $z \in B$, $z \neq 0$, and arbitrary $y \in A$.

Fixing an element $z \in B$, we can pass from f to the complex valued function $\eta_z \circ f : A \to T_b$. We can say that (3) is a decomposition of this function[1] with respect to the character group $\widehat{A}$. The functions of the form $A \to S_1(\mathbb{C})$ were already considered by Logachev, Sal'nikov, and Yashchenko (see Definition 4). We have [13, 24]

Theorem 12. *A function $f : A \to B$ is a bent function if and only if $\eta_z \circ f$ for every $z \neq 0$ is a bent function in sense of Logachev, Sal'nikov and Yashchenko.*

Refer as the *derivative of a function f in direction $y \in A$* to the function

$$D_y f(x) = f(x + y) - f(x).$$

We have [13, 24]

Theorem 13. *A function $f : A \to B$ is a bent function if and only if $D_y f(x)$ is a balanced function for every nonzero $y \in A$; i.e., the cardinalities of all its preimages are equal.*

Suppose that f is a bent function. Then, for every linear or affine permutation π on A, the function $f \circ \pi : A \to B$ is a bent function. If $\ell : B \to C$ is a surjective linear function (where C is a finite abelian group) then $\ell \circ f : A \to C$ is a bent function as well.

Solodovnikov defined [13] the *proximity* function of two functions $f, g : A \to B$ as

$$\delta(f, g) = \left(\frac{1}{m} \sum_{y \in B} \left(\frac{|\{x : f(x) - g(x) = y\}|}{n} - \frac{1}{m} \right)^2 \right)^{1/2}. \tag{4}$$

The intention is to use it to estimate the quality (or efficiency) of the replacement of one function with the other. The smaller the value of $\delta(f, g)$, the less close to each other f and g are. The definition of proximity implies that $\delta(f, g) = 0$ if and only if f and g differ by a balanced function.

Let $\mathrm{Hom}(A, B)$ denote the set of all group homomorphisms from A to B. By definition, for every homomorphism h, the derivative $D_y h(x)$ in every nonzero direction $y \in A$ is a constant function. Then it is natural to call [13] $f : A \to B$

[1] Here and below the expression $g \circ f(x)$ stands for the function $g(f(x))$.

such that $D_y f(x)$ is balanced for every nonzero $y \in A$ an *absolutely nonhomomorphic* function. By Theorem 13, absolutely nonhomomorphic functions and bent functions coincide.

Theorem 14. *Given a bent function f and a homomorphism h, we have*

$$\delta(f,h) = \frac{\sqrt{m-1}}{m\sqrt{n}}.$$

In other words, a bent function is equally close to all homomorphisms. It is interesting to consider *minimal functions*, which are the least close to homomorphisms, i.e., have the minimal value of $\delta_f = \delta(f, \mathrm{Hom}(A,B))$. For $A = \mathbb{Z}_q^\ell$ and $B = \mathbb{Z}_q^r$, it is shown in [13] that f is a minimal function if

$$\delta_f = \sqrt{m-1}/(m\sqrt{n}).$$

A function is called *absolutely minimal* if its minimality is invariant under all epimorphisms of the group B.

Theorem 15. *For prime q, take $A = \mathbb{Z}_q^\ell$ and $B = \mathbb{Z}_q^r$ and suppose that bent functions from A to B exist. Then*

(i) *every bent function is absolutely minimal;*

(ii) *for $q = 2$, the class of all bent functions coincides with the class of all absolutely minimal functions.*

For more on this topic, see [25]. It seems that soon some articles may appear dealing with the bent functions on finite nonabelian groups [49].

1.6. Vector G-Bent Functions

Solodovnikov suggested [13] the idea of this generalization of the functions $f : A \to B$. In 2004, L. Poinsot and S. Harari [50] considered it in detail for the case $A = \big(\mathbb{Z}_2^k, +\big)$ and $B = \big(\mathbb{Z}_2^r, +\big)$; i.e., for the Boolean vector functions. The generalization rests on the possibility of defining the derivative of a function $f : A \to B$ in a different fashion.

Let $S(A)$ denote the symmetric group on A in the multiplicative notation. A permutation $\sigma \in S(A)$ is called an *involution* whenever $\sigma\sigma = e$, where e is the identically permutation. A permutation σ has no *fixed points* if $\sigma(x) \neq x$ for every $x \in A$. Denote the set of all involutions σ without fixed points by $\mathrm{Inv}(A)$. A subgroup G of $S(A)$ with $G \subseteq \mathrm{Inv}(A) \cup \{e\}$ is called a *group of involutions of A*.

Suppose now that $A = \mathbb{Z}_2^k$ and $B = \mathbb{Z}_2^r$. Observe that

$$\big|\mathrm{Inv}\big(\mathbb{Z}_2^k\big)\big| = \frac{2^k!}{2^{k-1}!2^{2^{k-1}}}.$$

It is shown in [50] that every group of involutions G of $\mathbb{Z}_2^k$ is abelian and $|G| \leqslant 2^k$. We consider only a group G of the maximal order 2^k. A simple example of this group is the *translation group* $T\big(\mathbb{Z}_2^k\big)$ consisting of all permutations σ_y, $y \in \mathbb{Z}_2^k$, such that $\sigma_y(x) = x + y$. However, other maximal groups of involutions exist [50].

Take $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^r$ and a maximal group G of involutions of $\mathbb{Z}_2^k$. Refer as the *generalized derivative of f in direction $\sigma \in G$* to the function

$$D_\sigma f(x) = f(\sigma(x)) - f(x).$$

Note that if G is the translation group $T(\mathbb{Z}_2^k)$ then the generalized derivative coincides with the ordinary derivative $D_y f(x) = f(x+y) - f(x)$.

Definition 6 (Poinsot, Harari, 2004). Take $A = \big(\mathbb{Z}_2^k, +\big)$, $B = \big(\mathbb{Z}_2^r, +\big)$, and a maximal group G of involutions of A. A function $f : A \to B$ is called a *G-bent function* if the generalized derivatives $D_\sigma f(x)$ in every direction $\sigma \in G$, $\sigma \neq e$, are balanced.

In the interpretation of Solodovnikov, a G-bent function is a function f that can be changed by every permutation $\sigma \in G$, $\sigma \neq e$, as strongly as possible: $\delta(f, f \circ \sigma) = 0$.

A translation of the definition of G-bent functions into the language of generalized Fourier coefficients is proposed in [50], but so far it fails to appear thoroughly worked out and includes inaccuracies. Also it is unclear to what extent the approach of [50] applies if A and B are arbitrary abelian groups.

1.7. Multidimensional Bent Functions on a Finite Abelian Group

In 2005, L. Poinsot proposed [48] this direct generalization of the bent functions of Logachev, Sal'nikov, and Yashchenko [10].

Take the m-dimensional hermitian space $\mathbb{C}^m$ with the standard inner product

$$\langle x, y \rangle = \sum_{j=1}^{m} x_j \overline{y}_j,$$

the norm $\|x\|^2 = \langle x, x \rangle$, and the metric $d(x, y) = \|y - x\|$. Suppose that $S_1(\mathbb{C}^m)$ is the set of all points lying on the sphere of radius 1 centered at the origin.

As above, take a finite abelian group A of order n and its character group $\widehat{A} = \{\chi_y | y \in A\}$.

Refer as the *Fourier transform* of a function $f : A \to \mathbb{C}^m$ to the function

$$\widehat{f}(y) = \sum_{x \in A} f(x)\overline{\chi_y(x)}, \qquad \widehat{f} : A \to \mathbb{C}^m.$$

Definition 7 (Poinsot, 2005). Take a finite abelian group A of order n. A function $f : A \to S_1(\mathbb{C}^m)$ is called a *multidimensional bent function* if $\|\widehat{f}(y)\|^2 = n$ for every $y \in A$.

For $m = 1$, this definition is identical to Definition 4. Similarly, for multidimensional bent functions, we have Rothaus' criterion, define the dual multidimensional bent function, and so on [48]. However, so far it is unclear whether multidimensional bent functions can be of independent interest or are just a formal generalization of the bent functions of Definition 4.

2. Combinatorial generalizations of bent functions

In this section, we consider quite natural generalizations. We can say that each of them rests on a simple combinatorial idea.

2.1. Partially Defined Bent Functions

Given an arbitrary set $S \subseteq \mathbb{Z}_2^n$, take a *partially defined* Boolean function $f : S \to \mathbb{Z}_2$. Its *partial Walsh–Hadamard transform* is the mapping

$$W_{f,S}(y) = \sum_{x \in S} (-1)^{\langle x,y \rangle + f(x)} \quad \text{for every} \quad y \in \mathbb{Z}_2^n.$$

This transformation satisfies the analog of Parseval's equality:

$$\sum_{y \in \mathbb{Z}_2^n} W_{f,S}^2(y) = 2^n |S|.$$

Definition 8. A Boolean function f is called a *partially defined bent function* if

$$W_{f,S}(y) = \pm\sqrt{|S|} \quad \text{for every} \quad y \in \mathbb{Z}_2^n.$$

These functions are discussed in more detail in [12, Chap. 6]. Here we note only that so far it is unknown under what conditions on S partially defined bent functions exist.

2.2. Plateaued Functions

This generalization of bent functions is well-known, and we are very brief here.

Definition 9. A Boolean function is called *plateaued* if all its nonzero Walsh–Hadamard coefficients are equal in absolute value.

Parseval's equality implies that the nonzero coefficients must be of the form $\pm 2^{n-h}$ for some integer h with $0 \leqslant h \leqslant n$. The number of nonzero coefficients must be equal to 2^{2h}. The exponent $2h$ and the quantity 2^{n-h} are called respectively the *order* and *amplitude* of a plateaued function. The bent functions and the affine functions are the marginal particular cases of the plateaued functions (of orders n and 0 respectively).

For results on these functions, see the surveys [12, 23], as well as [27, 62, 63].

2.3. $\mathbb{Z}$-Bent Functions

In 2005, H. Dobbertin suggested [32] to study bent functions in the context of a more general approach which we can call recursive. We do not distinguish between an ordinary Boolean function $f(x)$ of $x \in \mathbb{Z}_2^n$ and the integer function $F(x) = (-1)^{f(x)}$. The *Fourier transform* of a function $F : \mathbb{Z}_2^n \to \mathbb{Z}$ is defined as

$$\widehat{F}(y) = \frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x,y \rangle} F(x).$$

Then a (± 1)-valued function F is a bent function if and only if $\widehat{F}$ is (± 1)-valued as well. The generalization goes as follows:

Definition 10 (Dobbertin, 2005). Given $T \subseteq \mathbb{Z}$, a function $F : \mathbb{Z}_2^n \to T$ is called a *T-bent function* if all values of $\widehat{F}$ belong to T.

Dobbertin chose the natural nested chain

$$T_0 = \{-1, +1\};$$
$$T_r = \{w \in \mathbb{Z} | -2^{r-1} \leqslant w \leqslant 2^{r-1}\}, \qquad r > 0.$$

A T_r-bent function is called a *$\mathbb{Z}$-bent function of level r*, and all these bent functions (for $r \in \mathbb{Z}$) constitute the class of *$\mathbb{Z}$-bent functions*. The possibilities of a recursive construction (decomposition) of $\mathbb{Z}$-bent functions by raising or lowering their level and the number of variables are studied in [32].

2.4. Homogeneous Bent Functions

This subclass of bent functions is isolated in [52] as consisting of the functions with relatively simple algebraic normal forms.

Definition 11 (C. Qu, J. Seberri, J. Pieprzyk, 2000). A bent function is called *homogeneous* if all monomials of its algebraic normal form are of the same degree.

Qu, Seberri, and Pieprzyk enumerated [52] all homogeneous bent functions of degree 3 of 6 variables (it turns out that there are exactly 30 of them) and posed the question of classifying the bent functions of this type with more variables. C. Charnes, M. Rotteler, and T. Beth proved [28] that there exist homogeneous bent functions of degree 3 of each number of variables $n > 2$.

T. Xia, J. Seberry, J. Pieprzyk, and C. Charnes established [59] that, for $n > 3$, there exist no homogeneous bent functions of n variables of the maximally possible degree $n/2$. Q. Meng, H. Zhang, M. C. Yang, and J. Cui showed [42, 43] that there exists no homogeneous bent functions of degree $(n/2) - 1$ for $n > 4$. But what is the sharp upper bound on the nonlinearity degree of a homogeneous bent function? Presently there is no answer to this question. There is only a conjecture [42] that, for every $k > 1$, there is $N \geqslant 2$ such that homogeneous bent functions of degree k of n variables exist for every $n > N$.

3. Cryptographic generalizations of bent functions

It is known that high nonlinearity alone is insufficient for good cryptographic functions. In this section, we consider some generalizations which arose from imposing additional restrictions on the set of Boolean functions.

3.1. Balanced Bent Functions

From the viewpoint of cryptography, the important criteria a Boolean function f of n variables must satisfy are as follows [11, 23]:

• *balancedness*, which means that f takes the values 0 and 1 equally often;

• order k *propagation criterion* $PC(k)$, which means that, for every nonzero vector $y \in \mathbb{Z}_2^n$ of weight at most k, where $1 \leqslant k \leqslant n$, the function $f(x+y)+f(x)$ is balanced [51];

• *maximal nonlinearity*, which means that f is such that the value of its nonlinearity N_f is maximal;

• *uniform correlation with linear functions*; the correlation between two functions f and g is defined as

$$c(f,g) = 1 - \frac{\operatorname{dist}(f,g)}{2^{n-1}};$$

for a function f the uniform correlation means that the value of $|c(f,g)|$ is constant for every linear function g.

However, these criteria contradict each other. Bent functions are maximally nonlinear, satisfy the criterion $PC(n)$, possess uniform correlation with linear functions (the value is equal to $\pm 2^{-n/2}$), but are not balanced. The following arises naturally:

Definition 12. A Boolean function f of n variables is called a *balanced bent function* if f is balanced and has the maximal possible nonlinearity.

It is established in [18] that if n is odd and f is a balanced function then

$$N_f \leqslant 2^{n-1} - 2^{(n-1)/2}.$$

In 1994, S. Chee, S. Lee, and K. Kim proposed [29] a method for constructing the balanced bent functions of odd numbers of variables possessing almost uniform correlation with the linear functions and satisfying the criterion $PC(k)$ for sufficiently large k. Let us present this method.

Given some odd n, take a nondegenerate binary $(n-1)\times(n-1)$ matrix A and a binary vector b of length $n-1$.

Theorem 16. *If f_0 is a bent function of $n-1$ variables and f_1 is the equivalent bent function*

$$f_1(x) = f_0(Ax+b)+1$$

then the function $g(x,z) = f_z(x)$ of n variables, where $x \in \mathbb{Z}_2^{n-1}$ and $z \in \mathbb{Z}_2$:

(i) *is a balanced bent function;*

(ii) *is an almost bent function (see the definition below);*

(iii) *has the only possible values* 0 *and* $\pm 2^{-(n-1)/2}$ *of correlation with a linear function;*

(iv) *satisfies the criterion PC for every nonzero vector $(y,0)$, where $y \in \mathbb{Z}_2^{n-1}$;*

(v) *satisfies the criterion $PC(n-1)$ if $A = E$ and b is a vector of all ones.*

3.2. Partially Bent Functions

As we have already noted, bent functions are neither balanced nor correlation immune. C. Carlet proposed [20] a new method to extend the class $\mathfrak{B}_n$ of functions enjoying these properties and having sufficiently high nonlinearity. These *partially bent functions* are defined using the following extremal property:

Denote the *autocorrelation* of a Boolean function f in direction y by

$$\Delta_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x)+f(x+y)}.$$

Let NW_f and $N\Delta_f$ denote the numbers of nonzero Walsh–Hadamard coefficients and autocorrelation coefficients of f respectively. Then [20] every Boolean function satisfies

$$NW_f \cdot N\Delta_f \geqslant 2^n.$$

Definition 13 (Carlet, 1993). A Boolean function f with $NW_f \cdot N\Delta_f = 2^n$ is called a *partially bent function*.

Theorem 17. *The following claims are equivalent:*

(i) *f is a partially bent function;*

(ii) *there exists a vector z such that, for every x, the value of the autocorrelation $\Delta_f(x)$ is equal to either 0 or $(-1)^{\langle x,z\rangle}2^n$;*

(iii) *there exist a vector z and a decomposition of $\mathbb{Z}_2^n$ into the direct sum of subspaces L and L' such that $f|_{L'}$ is a partially defined bent function (in the sense of Definition 8), and $f(x+y) = \langle x, z\rangle + f(y)$ for every $x \in L$ and $y \in L'$.*

Henceforth, z stands for the vector defined in Theorem 17. The subspace L for a partially bent function f is defined as the set of vectors x such that $\Delta_f(x) \neq 0$. We can equivalently define L as the space of linear structures of f; i.e., the space consisting of all vectors y with $f(x+y) + f(x) = \text{const}$. For a decomposition of $\mathbb{Z}_2^n$ into direct sum, the subspace L' is chosen arbitrarily. Observe that the dimension of L' must be even and denote it by $2h$. According to [20], we have the following results (for the necessary definitions see [12]):

Theorem 18. *A partially bent function f is*

(i) *balanced if and only if $f|_L \neq \text{const}$;*

(ii) *unbalanced of weight w if and only if $f|_L$ is a constant and $w = 2^{n-1} \pm 2^{n-h-1}$, where $\dim L = n - 2h$;*

(iii) *a plateaued function of order $2h$;*

(iv) *a correlation immune function of order k if and only if there is no vector of weight w, $1 \leqslant w \leqslant k$, in the dual class $z + L^\perp$;*

(v) *a balanced correlation immune function of order k if and only if there is no vector of weight at most k in the class $z + L^\perp$;*

(vi) *a function that satisfies the Propagation Criterion $PC(k)$ if and only if L does not include any vector of weight w, $1 \leqslant w \leqslant k$.*

Note that all affine, quadratic, and bent functions are partially bent functions.

The following is true [20]:

Theorem 19. *Let f be a partially bent function,* $\dim L = n - 2h$. *Then*

$$N_f = 2^{n-1} - 2^{n-h-1}, \qquad W_f(x) = \begin{cases} \pm 2^{n-h}, & \text{for } x \in z + L^\perp, \\ 0, & \text{otherwise.} \end{cases}$$

Obviously, the less the dimension of the space L, the higher is the nonlinearity of a partially bent function.

See further on this topic [23, 58].

3.3. Hyper-Bent Functions

In 2001, A. Youssef and G. Gong introduced [60] the concept of hyper-bent functions.[1] Previously, G. Gong and S. W. Golomb in 1999 considered [33] the DES ciphering algorithm as a nonlinear feedback shift register, and analyzed its S-blocks. For this approach the authors of [33] proposed to use proper monomial functions instead of linear Boolean functions for approximating the coordinate functions of the S-blocks. This idea was developed in [60].

We can regard a Boolean function of n variables as a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$, assigning to every vector x a corresponding element of the field $\mathbb{F}_{2^n}$. It is known that every linear function $\langle x, y\rangle$ can be expressed as $\mathrm{Tr}(a_x y)$ for suitable $a_x \in \mathbb{F}_{2^n}$, where $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the trace function. Then the Walsh–Hadamard transform assumes the equivalent form

$$W_f(y) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(yx)+f(x)}.$$

A function of the form $\mathrm{Tr}(a_x y^s)$, where the integer s satisfies $1 \leqslant s \leqslant 2^n - 1$ and $\gcd(s, 2^n - 1) = 1$, is called a *proper monomial function*.

The *extended Walsh–Hadamard transform* of a Boolean function f is

$$W_{f,s}(y) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(yx^s)+f(x)}.$$

Definition 14 (Youssef, Gong, 2001). A Boolean function f is called a *hyper-bent function* if $|W_{f,s}(y)| = 2^{n/2}$ for every $y \in \mathbb{F}_{2^n}$ and every integer s with $\gcd(s, 2^n - 1) = 1$. In other words, a hyper-bent function is equally badly approximated by all proper monomial functions; its generalized nonlinearity

$$\mathrm{NLG}(f) = 2^{n-1} - \frac{1}{2} \max_{y,s \in \{y,s \mid \gcd(s,2^n-1)=1\}} |W_{f,s}(y)|$$

is maximal: it is equal to $2^{n-1} - 2^{(n/2)-1}$.

For every even n, the authors of [60] proved the existence of hyper-bent functions, proposed their vector version, and considered balanced hyper-bent functions for small numbers of variables. In 2006, C. Carlet and P. Gaborit [26] and independently A. S. Kuz'min, V. T. Markov, A. A. Nechaev, and A. B. Shishkov [6] showed that the nonlinearity degree of every hyper-bent function of n variables is equal to $n/2$.

A. S. Kuz'min et al. [7, 8] generalize the concept of a hyper-bent function: from Boolean functions they pass to functions over an arbitrary finite field of characteristic 2:

Take $q = 2^\ell$. The problem of approximating arbitrary function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ (as above, it is identified with a function $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$) by functions of some bounded class $\mathcal{A}$ is considered in [8]. In order to estimate the efficiency of

[1] Prior to that the term *hyper-bent function* was used once in [21] for another class of functions, but that sense is not used anymore.

approximation of f by a function $g \in \mathcal{A}$, the *agreement* parameter $\nabla(f,g)$ was related to the proximity function of Solodovnikov (4) as

$$\nabla(f,g) = \frac{q}{\sqrt{q-1}}\delta(f,g)$$

if we choose the finite groups $A = (\mathbb{F}_{q^n}, +)$ and $B = (\mathbb{F}_q, +)$. This parameter appears more natural since $0 \leqslant \nabla(f,g) \leqslant 1$; and, for the marginal values 0 and 1, the functions f and g differ by a balanced function and a constant respectively. For $q = 2$, we have

$$\left|\mathbf{P}(f = g) - \frac{1}{2}\right| = \frac{\nabla(f,g)}{2};$$

thus, the less agreement there is between two functions, the lower the efficiency of replacing one with the other.

Let

$$\nabla(f,\mathcal{A}) = \max_{g\in\mathcal{A}} \nabla(f,g)$$

denote the *efficiency of approximation* of f by functions in $\mathcal{A}$.

• If $\mathcal{A} = \mathrm{Hom}(A,B)$ is the class of all homomorphisms from A to B then every function $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ such that $\nabla(f, \mathrm{Hom}(A,B))$ takes its minimal possible value $q^{-n/2}$ is a bent function in the sense of Definition 1.

• Suppose that $\mathcal{A} = \mathcal{M}$ is the class of all proper generalized monomial functions, i.e., the functions of the form $g(x) = h(x^s)$, where $h \in \mathrm{Hom}(A,B)$ and the integer s satisfies $\gcd(s, q^n - 1) = 1$.

Definition 15 (A. S. Kuz'min et al., 2007). A function $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is called a *hyper-bent function* if the parameter $\nabla(f,\mathcal{M})$ takes its minimal possible value $q^{-n/2}$.

For $q = 2$, Definitions 14 and 15 coincide.

A detailed study of these generalized hyper-bent functions appears in [7]. Let us present here only one construction of them. The multiplicative group of the field $\mathbb{F}_{q^n}$ is the direct product of $(\mathbb{F}_{q^{n/2}}, \cdot)$ and the cyclic group V of order $q^{n/2}+1$. Suppose that $z_{a,d}$ is equal to one (zero) for $a, d \in \mathbb{F}_q$ whenever a and d are equal (distinct).

Theorem 20. *Take a function $g : V \to \mathbb{F}_q$ such that there is $d \in \mathbb{F}_q$ for which the number of solutions to $g(x) = a$ in V is equal to $q^{(n/2)-1} + z_{a,d}$, where $a \in \mathbb{F}_q$. Then*

$$f : \mathbb{F}_{q^n} \to \mathbb{F}_q, \qquad f(0) = d, \qquad f(x) = g(x^{q^{n/2}-1}) \quad \textit{for} \quad x \neq 0$$

is a hyper-bent function.

For more on this topic, see [9, 61].

A. V. Ivanov also studied [3, 4] the monomial approximations of Boolean functions. For instance, he showed [5] that the property of a bent function to be hyper-bent in general depends on the choice of a basis for expressing it.

3.4. Near-Bent Functions

The bent functions exist only for even numbers of variables. For odd n, one of their analogs are the near-bent functions, which possess sufficiently high nonlinearity.

Definition 16. A Boolean function f of n variables is called a *near-bent function* if every Walsh–Hadamard coefficient of it is equal to either zero or $\pm 2^{(n+1)/2}$.

Near-bent functions are nothing but the plateaued functions of maximal order $n-1$ of odd number of variables, see Definition 9. We will not consider them in detail. Note only that the Boolean functions with three distinct values in the Walsh–Hadamard spectrum are interesting for defending against the so-called soft output joint attack on PN-generators [39] which are used in the standard IS–95 of CDMA technology. Near-bent functions are also used for constructing the cryptographically robust S-blocks [30].

For the near-bent functions, see [31, 38].

3.5. Bent Functions of Higher Nonlinearity Order

This is a quite natural direction closely related to nonlinear generalizations of various methods of cryptoanalysis.

It is known that the efficiency of approximating a bent function by linear functions is the lowest. Extending the class of linear functions, it is natural to consider for approximations the Boolean functions of degree at most r, where $2 \leqslant r \leqslant n-1$. This leads to the concept of *order r nonlinearity* $N_r(f)$ of a Boolean function f as the Hamming distance from f to all functions of this type.

Definition 17. A Boolean function at the maximal distance from all functions of degree at most r is called a *bent function of order r*.

The difficulty consists in determining this maximal possible value of $N_r(f)$. For $r \geqslant 2$, it is an open problem, better known in coding theory as the determination of the covering radius of the order r Reed–Muller code. Some estimates for $N_r(f)$ are known presently, as well as its asymptotic value, connections to other cryptographic parameters, and so on. For more details on this topic, see the 2008 survey by C. Carlet [22].

3.6. k-Bent Functions

In 2007, the author introduced [14] the following concept whose main idea is to consider approximating functions distinct from linear, but analogous to some extent.

Take binary vectors x and y of length n and an arbitrary integer k satisfying $1 \leqslant k \leqslant n/2$. Define the binary operation

$$\langle x, y\rangle_k = \left(\sum_{i=1}^{k} \sum_{j=i}^{k} (x_{2i-1} + x_{2i})(x_{2j-1} + x_{2j})(y_{2i-1} + y_{2i})(y_{2j-1} + y_{2j}) \right) + \langle x, y\rangle,$$

which serves as a nonlinear analog of the inner product. Observe that in this operation the components of the vectors are inequivalent: the first $2k$ components of each of them appear in both quadratic and linear terms, while the rest, only in the linear terms.

The function

$$W_f^{(k)}(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x,y\rangle_k + f(x)}$$

is called the *k-Walsh–Hadamard transform* of a Boolean function f. For $k = 1$, we have an expression equivalent to the ordinary Walsh–Hadamard transform. Parseval's equality

$$\sum_{y \in \mathbb{Z}_2^n} \left(W_f^{(k)}(y)\right)^2 = 2^{2n}$$

holds. A function f is called a *k-bent function with a fixed order of variables* if all its coefficients $W_f^{(j)}(y)$, $j = 1, \ldots, k$, are equal to $\pm 2^{n/2}$. These functions are considered in [14]. However, their drawback is the dependence on the order of variables. Let us present a more general definition, which is free from this drawback:

Definition 18. A Boolean function f of n variables is called a *k-bent function* if

$$W_{f\circ\pi}^{(j)}(y) = \pm 2^{n/2}.$$

for an arbitrary permutation $\pi \in S_n$, every $j = 1, \ldots, k$, and every vector y.

Let us explain this definition. Consider the set of functions

$$\mathfrak{A}_n^k(\pi) = \left\{ \langle \pi(x), y\rangle_k + a \mid y \in \mathbb{Z}_2^n,\ a \in \mathbb{Z}_2 \right\}$$

of n variables. The vectors of values of the functions of every class $\mathfrak{A}_n^k(\pi)$ constitute a binary Hadamard code. This code is nonlinear (for $k > 1$), but in the space $\mathbb{Z}_4^n$ there exists a linear preimage of it under a simple mapping, see [14] for more detail. Thus, we may regard the functions in $\mathfrak{A}_n^k(\pi)$ as analogs of affine functions. Observe that they are quadratic. Refer as the *k-nonlinearity* of a Boolean function f to the minimal Hamming distance $N_f^{(k)}$ from it to the set of all functions of the form $\langle \pi(x), y\rangle_k + a$, where π is an arbitrary permutation. We have

$$N_f^{(k)} = 2^{n-1} - \frac{1}{2} \max_{\pi \in S_n} \max_{y \in \mathbb{Z}_2^n} \left| W_{f\circ\pi}^{(k)}(y) \right|.$$

Therefore, a k-bent function is a function with maximal $N_f^{(j)}$; i.e., $N_f^{(j)} = 2^{n-1} - 2^{(n/2)-1}$, $j = 1, \ldots, k$. Thus, it is simultaneously maximally distant from all classes of functions $\mathfrak{A}_n^j(\pi)$, $\pi \in S_n$ and $j = 1, \ldots, k$. Observe that 1-bent functions coincide with ordinary bent functions. With the growth of k, the nonlinear properties of functions strengthen; thus, the most interesting problem apparently is to describe the class of all $(n/2)$-bent functions. As [14] implies, this class is nonempty. For every even n, it contains, for instance, all symmetric bent functions:

$$f(x) = \sum_{i=1}^{n} \sum_{j=i+1}^{n} x_i x_j,$$

and $f(x)+1$, $f(x)+\sum_{i=1}^{n} x_i$, $f(x)+\sum_{i=1}^{n} x_i+1$, which are characterized in [54].

For $n=4$, all $(n/2)$-bent functions are described in [16]. There are 128 quadratic functions with the quadratic part of one of four types:

$$x_1x_2+x_3x_4, \qquad x_1x_3+x_2x_4, \qquad x_1x_4+x_2x_3,$$
$$x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4,$$

and arbitrary linear part. See also [15] on this topic.

4. Quantum generalizations of bent functions

4.1. Negabent Functions, Bent$_4$ Functions, I-Bent Functions

A bent function is often defined as a function with a *flat spectrum* of the Walsh–Hadamard transform. Flatness means that the absolute values of all Walsh–Hadamard coefficients are equal. In 2006, C. Riera and M. G. Parker began to study [53] Boolean functions with flat spectra of a set of unitary transformations of a particular form. Recall that the transformation of the space $\mathbb{C}^n$ given by a square matrix A is *unitary* if $A\bar{A}^T=E$, where E is the identity matrix. These transformations are used in [53] for analyzing the stabilizers of quantum states. Put

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad N=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}.$$

For every 2×2 matrix A, let $A_j=I\otimes\cdots\otimes I\otimes A\otimes I\otimes\cdots\otimes I$ denote the tensor (Kronecker) product of n matrices, where A appears in position j. Consider the following sets of transformations:

- $\{H\}^n$ consisting of the transformations

$$U=\prod_{j=0}^{n-1} H_j.$$

If $F=(-1)^f$ is the *sign* function of a Boolean function f of n variables then the vector of spectral values of f with respect to the transformation U is defined as $\widehat{F}=UF$. Then f is a *bent function* (in the usual sense) if its spectrum with respect to U is flat; i.e., every component of $\widehat{F}$ is equal to ± 1.

- $\{N\}^n$ consisting of the transformations

$$U=\prod_{j=0}^{n-1} N_j.$$

Definition 19 (C. Riera and M. G. Parker, 2006). A Boolean function having flat spectrum with respect to U is called a *negabent function*.

Note that since U is a complex matrix, the definition of spectrum here involves certain specific features [46]. Every affine Boolean function is a negabent function.

M. G. Parker (2000, 2007) and A. Pott (2007) studied negabent functions in [45, 46]. The intersection of the classes of bent and negabent functions is under consideration in [46]; it is completely understood for quadratic functions.

- $\{H, N\}^n$ consisting of 2^n transformations of the form

$$\prod_{j \in R_H} H_j \prod_{j \in R_N} N_j,$$

where R_H and R_N partition the set $\{0, 1, \ldots, n-1\}$. A Boolean function f of n variables is a *bent$_4$-function* if there exists at least one partition R_H, R_N for which the spectrum of f is flat.

- $\{I, H\}^n$ consisting of 2^n transformations of the form

$$\prod_{j \in R_I} I_j \prod_{j \in R_H} H_j,$$

where R_I and R_H partition the set $\{0, 1, \ldots, n-1\}$. By analogy to the previous case, a function f is an *I-bent function* if there exists at least one partition R_I, R_H with $|R_I| < n$ for which the spectrum of f is flat.

- $\{I, H, N\}^n$ consisting of 3^n transformations

$$\prod_{j \in R_I} I_j \prod_{j \in R_H} H_j \prod_{j \in R_N} N_j,$$

where R_I, R_H, and R_N partition $\{0, 1, \ldots, n-1\}$. In this case we may define the so-called *I-bent$_4$ functions* which however are of little interest since this class includes all Boolean functions.

Riera and Parker [53] develop the quantum direction of their research, study the properties of the bent functions of the new type, and their connections to graphs.

Acknowledgments

I am grateful to the referee for attentively reading the article and making useful comments.

The author was supported by the Grant of the President of the Russian Federation for Young Russian Researchers (project no. MK–1250.2009.1), the Russian Foundation for Basic Research (projects nos. 08–01–00671 and 09–01–00528), and the Federal Target Program "Scientific and Educational Personnel of Innovative Russia" for 2009–2012 (State contract no. 02.740.11.0429).

References

[1] D. V. Ageev, "Bases of the Theory of Linear Selection. Code Demultiplexing," in *Proceedings of the Leningrad Experimental Institute of Communication* (Experimental Institute of Communication, Leningrad, 1935), pp. 3–35.

[2] A. C. Ambrosimov, "Properties of the Bent Functions of q-Ary Logic over Finite Fields," Discrete Math. **6** (3), 50–60 (1994).

[3] A. V. Ivanov, "Using Some Reduced Representation of the Boolean Functions Under Constructing Their Nonlinear Approximations," Vestnik Tomsk. Gos. Univ. Suppl. No. 23, 31–35 (2007).

[4] A. V. Ivanov, "Approximation of the Plateaued Boolean Functions by Monomial Functions," Prikl. Diskret. Mat. **1** (1), 10–14 (2008).

[5] A. V. Ivanov, "The Degree of Proximity of the Boolean Function Reduced Representation to the Class of Monomial Functions According to Basis Selection," Prikl. Diskret. Mat. Suppl. No. 1, 7–9 (2009).

[6] A. S. Kuz'min, V. T. Markov, A. A. Nechaev, and A. B. Shishkov, "Approximation of Boolean Functions by Monomial Functions," Diskret. Mat. **18** (1), 9–29 (2006).

[7] A. S. Kuz'min, A. A. Nechaev, and V. A. Shishkin, "Bent- and Hyperbent Functions over the Finite Field," Trudy Diskret. Mat. **10**, 97–122 (2007).

[8] A. S. Kuz'min, V. T. Markov, A. A. Nechaev, V. A. Shishkin, and A. B. Shishkov, "Bent- and Hyperbent Functions Over the Field of 2^ℓ Elements," Problemy Peredachi Informatsii **44** (1), 15–37 (2008) [Problems Inform. Transmission **44** (1), 12–33 (2008)].

[9] A. S. Kuz'min, A. A. Nechaev, and V. A. Shishkin, "Parameters of (Hyper-) Bent Functions Over the Field of 2^l Elements," Trudy Diskret. Mat. **11**, 47–59 (2008).

[10] O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko, "Bent Functions Over a Finite Abelian Group," Diskret. Mat. **9** (4), 3–20 (1997).

[11] O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko, "Cryptographic Properties of Discrete Functions," in *Proceedings of the Conference "Moscow State University and Development of Cryptography in Russia," Moscow State University,* 2002 (MTsNMO, Moscow, 2003), pp. 174–199.

[12] O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptology* (MTsNMO, Moscow, 2004).

[13] V. I. Solodovnikov, "Bent Functions from a Finite Abelian Group to a Finite Abelian Group," Diskret. Mat. **14** (1), 99–113 (2002).

[14] N. N. Tokareva, "Bent Functions with Stronger Nonlinear Properties: k-Bent Functions," Diskret. Anal. Issled. Oper. Ser. 1, **14** (4), 76–102 (2007) [J. Appl. Indust. Math. **2** (4), 566–584 (2008)].

[15] N. N. Tokareva, "On Quadratic Approximations in Block Ciphers," Problemy Peredachi Informatsii **44** (3), 105–127 (2008) [Problems Inform. Transmission **44** (3), 266–286 (2008].

[16] N. N. Tokareva, "Description of k-Bent Functions in Four Variables," Diskret. Anal. Issled. Oper. **15** (4), 74–83 (2008) [J. Appl. Indust. Math. **3** (2), 284–289 (2009)].

[17] N. N. Tokareva, "The Bent Functions: Results and Applications. An Overview," Prikl. Diskret. Mat. **2** (1), 15–37 (2009) [`http://mi.mathnet.ru/pdm50`].

[18] C. Adams and S. Tavares, "The Structured Design of Cryptographycally Good S-Boxes," J. Cryptology **3** (1), 27–43 (1990).

[19] S. V. Agievich, "Bent rectangles," in *NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security* (*Zvenigorod, Russia. September* 8–18*,* 2007)*. Proceedings* (IOS Press, Netherlands, 2008), pp. 3–22 [`http://arxiv.org/abs/0804.0209`].

[20] C. Carlet, "Partially-Bent Functions," Des. Codes Cryptography **3** (2), 135–145 (1993).

[21] C. Carlet, "Hyper-Bent Functions," in *International Conference on the Theory and Applications of Cryptology PRAGOCRYPT*'96 (Czech Tech. Univ. Publ. House, Prague, 1996), pp. 149–155.

[22] C. Carlet, "On the Higher Order Nonlinearities of Boolean Functions and S-Boxes, and Their Generalizations," in 5*th International Conference on Sequences and Their Applications SETA*'2008 (*Lexington, Kentucky, USA. September* 14–18*,* 2008). *Proceedings* (Springer, Berlin, 2008), pp. 345–367 [*Lectures Notes in Computer Science*, Vol. 5203].

[23] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes," in *Boolean Methods and Models*, Ed. by P. Hammer and Y. Crama (Cambridge Univ. Press, Cambridge, to appear) [`www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`].

[24] C. Carlet and C. Ding, "Highly Nonlinear Mappings," J. Complexity **20** (2–3), 205–244 (2004).

[25] C. Carlet and C. Ding, "Nonlinearities of S-Boxes," Finite Fields Appl. **13** (1), 121–135 (2007).

[26] C. Carlet and P. Gaborit, "Hyper-Bent Functions and Cyclic Codes," J. Comb. Theory. Ser. A. **113** (3), 466–482 (2006).

[27] C. Carlet and E. Prouff, "On Plateaued Functions and Their Constructions," in *Fast Software Encryption FSE*'2003*,* 10*th International Workshop (Lund, Sweden. February* 24–26*,* 2003)*. Proceedings* (Springer, Berlin, 2003), pp. 54–73 [*Lecture Notes in Computer Science*, Vol. 2887].

[28] C. Charnes, M. Rotteler, and T. Beth, "Homogeneous Bent Functions, Invariants, and Designs," Des. Codes Cryptography **26** (1–3), 139–154 (2002).

[29] S. Chee, S. Lee, and K. Kim, "Semi-Bent Functions," in *Advances in Cryptology—ASIACRYPT*'94*.* 4*th International Conference on the Theory and Applications of Cryptology* (*Wollongong, Australia. November* 28–*December* 1*,* 1994)*. Proceedings* (Springer, Berlin, 1995), pp. 107–118 [*Lecture Notes in Computer Science*, Vol. 917].

[30] J. Detombe and S. Tavares, "Constructing Large Cryptographically Strong S-Boxes," in *Advances in Cryptology—AUSCRYPT'92* (*Gold Coast, Queensland, Australia. December* 13–16*,* 1992). *Proceedings* (Springer, Berlin, 1993), pp. 165–181 [*Lecture Notes in Computer Science*, Vol. 718].

[31] J. F. Dillon and G. McGuire, "Near Bent Functions on a Hyperplane," Finite Fields Appl. **14**, 715–720 (2008).

[32] H. Dobbertin and G. Leander, "Cryptographer's Toolkit for Construction of 8-Bit Bent Functions," Cryptology ePrint Archive, Report 2005/089 (`http://eprint.iacr.org/`).

[33] G. Gong and S. W. Golomb, "Transform Domain Analysis of DES," IEEE Trans. Inform. Theory **45** (6), 2065–2073 (1999).

[34] T. Helleseth and A. Kalosha, "Monomial and Quadratic Bent Functions Over the Finite Fields of Odd Characteristic," Reports in Informatics, 2005. Report 310. (University of Bergen, Bergen, 2005).

[35] X. D. Hou, "q-Ary Bent Functions Constructed from Chain Rings," Finite Fields Appl. **4** (1), 55–61 (1998).

[36] X. D. Hou, "p-Ary and q-Ary Versions of Certain Results About Bent Functions and Resilient Functions," Finite Fields Appl. **10** (4), 566–582 (2004).

[37] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized Bent Functions and Their Properties," J. Comb. Theory Ser. A, **40** (1), 90–107 (1985).

[38] N. G. Leander and G. McGuire, "Construction of Bent Functions from Near-Bent Functions," J. Comb. Theory Ser. A, **116** (4), 960–970 (2009).

[39] S. Leveiller, G. Zemor, P. Guillot, and J. Boutros, "A New Cryptanalytic Attack for PN-Generators Filtered by a Boolean Function," in *Selected Areas of Cryptography—SAC'*2002 (*Newfoundland, Canada, August* 15–16*,* 2002). *Proceedings* (Springer, Berlin, 2003), pp. 232–249 [*Lecture Notes in Computer Science*, Vol. 2595].

[40] R. L. McFarland, "A family of Difference Sets in Noncyclic Groups," J. Comb. Theory, Ser. A **15** (1), 1–10 (1973).

[41] S. Matsufuji and K. Imamura, "Real-Valued Bent Functions and Their Application to the Design of Balanced Quadriphase Sequences With Optimal Correlation Properties," in *International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes—AAECC*−8 (*Tokyo, Japan. August* 20–24*,* 1990). *Proceedings* (Springer, Berlin, 1990), pp. 106–112 [*Lecture Notes in Computer Science*, Vol. 508].

[42] Q. Meng, H. Zhang, M. C. Yang, and J. Cui, "On the Degree of Homogeneous Bent Functions," `http://eprint.iacr.org`, 2004/284.

[43] Q. Meng, H. Zhang, M. C. Yang, and J. Cui, "On the Degree of Homogeneous Bent Functions," Discret. Appl. Math. **155** (5), 665–669 (2007).

[44] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent Function Sequences," IEEE Trans. Inform. Theory **28** (6), 858–864 (1982).

[45] M. G. Parker, "The Constabent Properties of Golay–Davis–Jedwab Sequences," in *IEEE International Symposium on Information Theory—ISIT'*2000 (*Sorrento, Italy. June* 25–30*,* 2000). *Proceedings* (Institute of Electrical and Electronics Engineers, New York, 2000), pp. 302.

[46] M. G. Parker and A. Pott, "On Boolean Functions Which Are Bent and Negabent," in *Sequences, Subsequences, and Consequences—SSC'*2007*. International Workshop* (*Los Angeles, CA, USA. May* 3*–June* 2*,* 2007)*. Proceedings* (Springer, Berlin, 2007), pp. 9–23 [*Lecture Notes in Computer Science*, Vol. 4893].

[47] K. G. Paterson, "On Codes with Low Peak-to-Average Power Ratio for Multicode CDMA," IEEE Trans. Inform. Theory **50** (3), 550–558 (2004).

[48] L. Poinsot, "Multidimensional Bent Functions," GESTS Intern. Transactions on Comput. Sci. Eng. **18** (1), 185–195 (2005).

[49] L. Poinsot and S. Harari, "Nonabelian Bent Functions," IEEE Trans. Inform. Theory, to appear (`http://poinsot.univ-tln.fr/publi.html`).

[50] L. Poinsot and S. Harari, "Generalized Boolean Bent Functions," in *Progress in Cryptology—Indocrypt'*2004 (*Chennai* (*Madras*)*, India. December* 20–22*,* 2004)*. Proceedings* (Springer, Berlin, 2005), pp. 107–119 [*Lecture Notes in Computer Science*, Vol. 3348].

[51] B. Preneel, W. van Leekwijck, L. van Linden, R. Govaerts, and J. Vandevalle, "Propagation Characteristics of Boolean Functions," in *Advances in Cryptology—EUROCRYPT'*1990*. International Conference on the Theory and Application of Cryptographic Techniques* (*Aarhus, Denmark. May* 21–24*,* 1990)*. Proceedings* (Springer, Berlin, 1991), pp. 161–173 [*Lecture Notes in Computer Science*, Vol. 473].

[52] C. Qu, J. Seberry, and J. Pieprzyk, "Homogeneous Bent Functions," Discrete Appl. Math. **102** (1-2), 133–139 (2000).

[53] C. Riera and M. G. Parker, "Generalized Bent Criteria for Boolean Functions (I)," IEEE Trans. Inform. Theory **52** (9), 4142–4159 (2006).

[54] P. Savicky, "On the Bent Boolean Functions That Are Symmetric," European J. Comb. **15** (4) 407–410 (1994).

[55] K.-U. Schmidt, "Quaternary Constant-Amplitude Codes for Multicode CDMA," in *IEEE International Symposium on Information Theory—ISIT'*2007 (*Nice, France. June* 24–29*,* 2007)*. Proceedings* (2007), pp. 2781–2785 (`http://arxiv.org/abs/cs.IT/0611162`).

[56] P. Solé and N. Tokareva, "Connections Between Quaternary and Binary Bent Functions," Cryptology ePrint Archive, Report 2009/544 (`http://eprint.iacr.org`).

[57] T. Wada, "Characteristic of Bit Sequences Applicable to Constant Amplitude Orthogonal Multicode systems," IEICE Trans. Fundamentals **E83-A** (11), 2160–2164 (2000).

[58] X. Wang and J. Zhou, "Generalized Partially Bent Functions," in *Future Generation Communication and Networking* (*Jeju-Island, Korea. December* 6–9*,* 2007)*. Proceedings* (2007), pp. 16–21.

[59] T. Xia, J. Seberry, J. Pieprzyk, and C. Charnes, "Homogeneous Bent Functions of Degree n in $2n$ Variables Do Not Exist for $n > 3$," Discrete Appl. Math. **142** (1–3), 127–132 (2004).

[60] A. Youssef and G. Gong, "Hyper-Bent Functions," in *Advanced Cryptology—EUROCRYPT*'2001*: International Conference on the Theory and Application of Cryptographic Techniques* (*Innsbruk, Austria, May* 6–10*,* 2001)*. Proceedings* (Berlin, Springer, 2001), pp. 406–419 [*Lecture Notes in Computer Science*, Vol. 2045].

[61] A. M. Youssef, "Generalized Hyper-Bent Functions over $GF(p)$," Discrete Appl. Math. **155** (8), 1066–1070 (2007).

[62] Y. Zheng and X.-M. Zhang, "Relationships Between Bent Functions and Complementary Plateaued Functions," in *International Conference on Information Security and Cryptology ICISC*'99 (*Seoul, Korea, December* $9-10$*,* 1999)*. Proceedings* (Berlin, Springer, 2000), pp. 60–75 [*Lecture Notes in Computer Science*, Vol. 1787].

[63] Y. Zheng and X.-M. Zhang, "On Plateaued Functions," IEEE Trans. Inform. Theory **47** (3), 1215–1223 (2001).